Bennett-Carper Data Security Act of 2006
Frequently Asked Questions

Who is covered by the Data Security Act of 2006?

Financial institutions, their affiliates and any other entities engaged in any financial activities described in Section 4(k) of the Bank Holding Company Act.

Any other entity, including federal agencies, that maintains or communicates covered information.

What types of information are covered?

Any information that could be used to commit identity theft or account fraud would be covered.

Sensitive personal information – first and last name, address or telephone number, in combination with 1. Social Security Number (SSN), 2. Drivers License Number (DLN), or 3.Taxpayer Identification Number (TIN). There is an exception for publicly available information.

Sensitive account information – financial account numbers relating to a consumer, including a credit or debit card number, in combination with any security code, access code, password or other personal identification information required to access the financial account.

What are the safeguarding or security requirements of covered entities?

All covered entities would be required to put in safeguards to protect all sensitive personal or account information.

The functional regulators would craft the detailed safeguarding requirements for their covered entities based upon the size and the complexity of the entity and the sensitivity of the consumer information.

Are electronic and paper records covered?

Both electronic and paper records are covered.

What is the trigger for consumer notification of a breach?

The trigger would be based on the likelihood that the breach of information will lead to "substantial harm or inconvenience" due to identity theft or account fraud.

"**Substantial harm or inconvenience**" includes identity theft or account fraud situations where consumers experience financial loss

or are forced to expend significant time and effort to correct false information.

Broad consumer notice would not be required if the information stolen was not useable to the thief, through encryption for example, or if it is not enough to steal someone's identity or engage in fraudulent credit card, debit card or other transactions. For instance, notice would not be required in a situation where the consumer merely receives a replacement credit or debit card since there was no financial loss and little if any inconvenience.

How will notification work?

Functional regulators would prescribe regulations regarding method, content and timing of notifications required to consumers.

What is a functional regulator?

The state or federal entity charged to oversee operations and business practices of covered entities.

For example, FDIC, Federal Reserve, and OCC would oversee most financial institutions. Other entities will fall within the enforcement jurisdiction of Federal Trade Commission (FTC). Federal agencies are internally regulated.

Is there a preemption of existing state laws?

All state laws relating to security and breach notification are preempted to create a uniform national standard.

Although some of these laws contain similar elements, many have inconsistent and conflicting standards. Different state laws result in higher costs and uneven consumer protection. The need to track multiple state laws is particularly difficult for smaller institutions and could lead to consumer delays in receiving timely notices.

Who will enforce this law?

The bill is based upon the GLB model and will be enforced exclusively by the functional regulator of the covered entity.

Why is there a safe harbor for some financial institutions?

Many financial institutions already have a safeguarding requirement and breach notification regime in place under GLB law, regulations and guidance. It is a system that is working and is in fact the model for this legislation. There is no need to rewrite those laws or regulations as they relate to safeguarding or breach notification.

DATA SECURITY ACT OF 2006
SPONSORED BY SEN. BOB BENNETT AND SEN. TOM CARPER
SUMMARY
JUNE 23, 2006

COVERED ENTITIES

- Covers entities in the business of engaging in financial activities under section 4(k) of the Bank Holding Company Act and financial institutions.
- Also covers entities that maintain or possess information subject to the Fair Credit Reporting Act's disposal rule and any other entities that maintain or communicate sensitive personal or account information.
- Agencies are subject to separate safeguarding and notification duties.

COVERED INFORMATION

- Sensitive personal information – first and last name, address or telephone number, in combination with (1) SSN, (2) DLN, or (3) TIN. Excludes publicly available information.
- Sensitive account information – financial account number relating to a consumer, including a credit or debit card number, in combination with any security code, access code, password or other personal identification information required to access the financial account.
- Not limited to *customer* information.
- Includes paper as well as computerized data.

DATA SECURITY

- Covered entity must implement and maintain reasonable policies and procedures to protect the confidentiality and security of sensitive account and personal information maintained or communicated by or on behalf of such entity from unauthorized use that is reasonably likely to result in substantial harm or inconvenience to the consumer.
- Allows flexibility in customizing policies and procedures.

INVESTIGATION

- Following a security breach, covered entity must assess the nature and scope of the breach, identify any sensitive account or personal information involved in the breach, determine if such information is reasonably likely to be misused in a manner causing substantial harm or inconvenience to consumers.
- Covered entity to consider whether any neural network or security program has or will detect account fraud.

TRIGGER FOR NOTIFICATION

- Covered entities must notify if the information involved in a security breach is reasonably likely to be misused in a manner causing substantial harm or inconvenience to consumers.
- Exempts from definition of security breach information that is not usable to commit identity theft or account fraud, including information that is encrypted or redacted.

- Specifies that substantial harm or inconvenience does not include changing an account number or closing an account, nor harm or inconvenience resulting from something other than identity theft or account fraud (*e.g.* embarrassment).

BIFURCATED APPROACH TO NOTIFICATION

- Covered entity must notify (1) its functional regulator, (2) law enforcement, (3) the account-holding institution if the breach involves sensitive account information, (4) nationwide credit reporting agencies (CRAs) if the breach involves sensitive personal information and the number of affected individuals exceeds 5,000, and (5) affected consumers.

PREEMPTION

- Preempts state laws imposing obligations to: (1) protect the security of information relating to consumers; (2) safeguard information relating to consumers from potential misuse; (3) investigate or provide notice of unauthorized access to information relating to consumers or potential misuse of such information for fraudulent, illegal, or other purposes; or (4) mitigate any loss or harm resulting from unauthorized access or misuse of information relating to consumers.

SAFE HARBOR

- Financial institution deemed in compliance with safeguarding obligation if it maintains policies and procedures consistent with section 501(b) of GLB that cover non-customer as well as customer information.
- Financial institution deemed in compliance with investigation and notification obligations if it maintains policies and procedures consistent with section 501(b) of GLB that include investigation and notification to law enforcement, owners of financial accounts and CRAs as well as consumers.

ENFORCEMENT

- As in GLB, enforcement limited to functional regulators.
- Includes OFHEO as functional regulator for GSEs.
- Explicitly prohibits private rights of action.

RULEMAKING

- Functional regulators to prescribe content, method and timing of notice and allow delay for law enforcement reasons.
- Required consultation and coordination among functional regulators in issuing rules.

SERVICE PROVIDERS

- Regulations to require service providers to notify entity on whose behalf they are maintaining or communicate information following a security breach.
- Regulations also ensure that there is only one notification responsibility with respect to a security breach.

Senator Bob Bennett
Introduction of The Data Security Act of 2006
Opening Statement
June 23, 2006

Mr. President, I rise today with my friend and colleague on the Banking Committee, the Senator from Delaware, Mr. Carper, to introduce legislation that I believe is of great importance to our economy and to American consumers. This legislation, The Data Security Act of 2006, will help protect individuals and businesses from the crimes of identity theft and account fraud, which are increasing at an alarming rate. These crimes impose higher costs on every consumer and business and can be financially debilitating to individuals whose personal information is stolen.

We are now living in the Information Age. Information drives our economy from the design and production phase of new products or services to payment and delivery. Information technology and electronic networks have brought conveniences and efficiencies to both producers and consumers in our economy. Producers can better focus their products and services to potential customers and consumers get the products they want with multiple payment options. Technology and, specifically, information technology makes this process ever more convenient and efficient.

All of the conveniences and efficiencies of the Information Age which benefit our evolving economy and its consumers have also brought new challenges. Criminals have also entered the Information Age and are now targeting and using information technology to steal from many of us.

Information databases and electronic information networks that contain sensitive personal information and sensitive financial account information are increasingly targets of sophisticated hackers, organized crime rings, identity thieves, and other criminals. When an individual has his identity or account information stolen from one of these sources and criminals use his or her legitimate name and credit history to create fraudulent accounts, or fraudulently access an existing account, by the time it is discovered, it is often too late to prevent that consumer from the need to invest significant time and effort to clear his or her name. These crimes also impose significant costs on financial institutions which are often liable for the loss of funds from the fraud. These costs are then passed on to all consumers through higher prices. We need to do more to prevent this type of fraud from happening in the first instance.

Currently, we are only partially protecting consumers from account fraud and identity theft. Criminals have shown they know how to exploit any weakness in information databases and networks, so we must do more to protect this

information regardless of where it is located. Most of the recent data security breaches have occurred outside of financial institutions.

The Gramm-Leach-Bliley Act requires financial institutions to protect the security and confidentiality of customer information. The federal banking agencies have issued guidance under the Gramm-Leach-Bliley Act requiring banks to investigate and provide notices to customers of breaches of data security involving customer information that could lead to account fraud or identity theft. Even with GLB and the associated regulations and guidance that have been implemented, many databases and information networks continue to be vulnerable because federal law generally does not require entities that are not financial institutions to protect the security and confidentiality of sensitive information relating to consumers, or to investigate and provide notices to consumers of breaches that may lead to account fraud or identity theft.

I recognize that many states have enacted security breach notification statutes in an effort to protect their citizens and I commend them for their efforts, but these statutes impose different and sometimes conflicting requirements, thereby providing consumers with uneven protection and subjecting businesses to multiple and confusing standards.

Our credit granting system and financial payments system is a national one and not a state based system. Consumers generally benefit greatly because of our national system. Because of that fact, I believe we need a national uniform system governing data security and security breach notification for financial institutions and other entities that maintain or communicate financial account information or personally identifiable information that could be used by identity thieves.

The standards established as a result of the guidance issued by the federal banking agencies under the Gramm-Leach-Bliley Act provide an appropriate model for federal data security and security breach notification requirements and is, therefore, the model for The Data Security Act of 2006.

The Data Security Act of 2006 will provide a uniform national standard for data security and breach notification. Sensitive personal and account information must be protected, and in the event where that protection is breached and there is a risk to the individual of identity theft or account fraud, that individual must be notified so that he or she can take the appropriate steps to protect him or her self.

I encourage my colleagues to closely review this legislation and I hope we can act quickly here in the Senate to pass The Data Security Act of 2006. I thank my friend from Delaware, Senator Carper, for joining with me today to introduce this legislation.